10/665,184

4

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１１月２５日

出 願 番 号
Application Number: 特願２００２－３４１２２２

[ST. 10/C]: [ＪＰ２００２－３４１２２２]

出 願 人
Applicant(s): 株式会社リコー

２００３年 ７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０５７７４５

【書類名】　特許願

【整理番号】　0206285

【提出日】　平成14年11月25日

【あて先】　特許庁長官　太田　信一郎　殿

【国際特許分類】　G06F 13/00

H04N　1/44

【発明の名称】　ドキュメントセキュリティプロファイル方法、及びその方法における処理を行う入出力装置、入出力装置アダプタ、入出力装置ドライバプログラム

【請求項の数】　24

【発明者】

【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内

【氏名】　斉藤　敦久

【特許出願人】

【識別番号】　000006747

【氏名又は名称】　株式会社リコー

【代理人】

【識別番号】　100070150

【弁理士】

【氏名又は名称】　伊東　忠彦

【手数料の表示】

【予納台帳番号】　002989

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　　ドキュメントセキュリティプロファイル方法、及びその方法における処理を行う入出力装置、入出力装置アダプタ、入出力装置ドライバプログラム

【特許請求の範囲】

【請求項１】　入出力装置との文書のセキュリティに関する情報の送受信を制御するドキュメントセキュリティプロファイル方法であって、

第１の入出力装置から受信した文書のセキュリティに関する文書属性情報に基づいて、上記文書のコンテンツに埋め込まれる埋め込み情報を上記第１の入出力装置に送信する第１送受信手順と、

第２の入出力装置から受信した上記埋め込み情報に基づいて、上記文書属性情報を上記第２の入出力装置に送信する第２送受信手順とを有することを特徴とするドキュメントセキュリティプロファイル方法。

【請求項２】　上記文書を識別する識別情報に対応付けて上記文書属性情報と上記埋め込み情報とを文書情報として管理する文書情報管理手順を有し、

上記第１送受信手順は、上記文書情報に基づいて上記埋め込み情報を上記第１の入出力装置に送信し、

上記第２送受信手順は、上記文書情報に基づいて上記文書属性情報を上記第２の入出力装置に送信することを特徴とする請求項１記載のドキュメントセキュリティプロファイル方法。

【請求項３】　上記埋め込み情報は、上記文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であることを特徴とする請求項１又は２記載のドキュメントセキュリティプロファイル方法。

【請求項４】　文書のコンテンツ情報を入出力する入出力装置であって、

上記文書を処理する文書処理手段から上記文書のコンテンツ情報の出力を指示する指示情報を受信する指示情報受信手段と、

上記指示情報に基づいて上記文書のセキュリティに関する文書属性情報を抽出する抽出手段と、

上記文書属性情報に対応する上記文書のコンテンツに埋め込まれる埋め込み情

報を取得する取得手段と、

上記埋め込み情報と共に上記文書のコンテンツ情報を出力する出力手段とを有することを特徴とする入出力装置。

【請求項５】　上記取得手段は、上記文書属性情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、

上記管理手段から送信された上記文書属性情報に対応する上記埋め込み情報を受信する受信手段とを有することを特徴とする請求項４記載の入出力装置。

【請求項６】　上記埋め込み情報は、上記文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であることを特徴とする請求項４又は５記載の入出力装置。

【請求項７】　文書のコンテンツ情報を入出力する入出力装置であって、

上記文書のコンテンツ情報が出力された媒体から該文書のコンテンツ情報を読み取る読取手段と、

上記文書のコンテンツ情報に埋め込まれた埋め込み情報を抽出する抽出手段と、

上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を取得する取得手段と、

上記文書属性情報に基づいて上記文書に関する処理を制御する制御手段とを有することを特徴とする入出力装置。

【請求項８】　上記取得手段は、上記埋め込み情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、

上記管理手段から送信された上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を受信する受信手段とを有することを特徴とする請求項７記載の入出力装置。

【請求項９】　上記文書を識別する識別情報に対応付けて上記文書属性情報と上記埋め込み情報とを文書情報として管理する文書情報管理手段を有することを特徴とする請求項７記載の入出力装置。

【請求項１０】　上記埋め込み情報は、上記文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であることを特徴と

する請求項７乃至９いずれか一項記載の入出力装置。

【請求項１１】　文書のセキュリティに関する情報の送受信を行う入出力装置アダプタであって、

上記文書を処理する文書処理手段から上記文書のコンテンツ情報の出力を指示する指示情報を受信する指示情報受信手段と、

上記指示情報に基づいて上記文書のセキュリティに関する文書属性情報を抽出する抽出手段と、

上記文書属性情報に対応する上記文書のコンテンツに埋め込まれる埋め込み情報を取得する取得手段と、

上記埋め込み情報を上記文書のコンテンツ情報を入出力する入出力装置へ送信する埋め込み情報送信手段とを有することを特徴とする入出力装置アダプタ。

【請求項１２】　上記取得手段は、上記文書属性情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、

上記管理手段から送信された上記文書属性情報に対応する上記埋め込み情報を受信する受信手段とを有することを特徴とする請求項１１記載の入出力装置アダプタ。

【請求項１３】　文書のセキュリティに関する情報の送受信を行う入出力装置ドライバプログラムであって、

上記文書を処理する文書処理手段から上記文書のコンテンツ情報の出力を指示する指示情報を受信する指示情報受信手順と、

上記指示情報に基づいて上記文書のセキュリティに関する文書属性情報を抽出する抽出手順と、

上記文書属性情報に対応する上記文書のコンテンツに埋め込まれる埋め込み情報を取得する取得手順と、

上記埋め込み情報を上記文書のコンテンツ情報を入出力する入出力装置へ送信する埋め込み情報送信手順とを有することを特徴とする入出力装置ドライバプログラム。

【請求項１４】　上記取得手順は、上記文書属性情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手順と、

上記管理手段から送信された上記文書属性情報に対応する上記埋め込み情報を受信する受信手順とを有することを特徴とする請求項１３記載の入出力装置ドライバプログラム。

【請求項１５】　文書のセキュリティに関する情報の送受信を行う入出力装置アダプタであって、

上記文書のコンテンツ情報が出力された媒体から該文書のコンテンツ情報を読み取る読取手段と、

上記文書のコンテンツ情報に埋め込まれた埋め込み情報を抽出する抽出手段と、

上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を取得する取得手段と、

上記文書属性情報を上記文書のコンテンツ情報を入出力する入出力装置へ送信する文書属性情報送信手段とを有することを特徴とする入出力装置アダプタ。

【請求項１６】　上記取得手段は、上記埋め込み情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、

上記管理手段から送信された上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を受信する受信手段とを有することを特徴とする請求項１５記載の入出力装置アダプタ。

【請求項１７】　文書のセキュリティに関する情報の送受信を行う入出力装置ドライバプログラムであって、

上記文書のコンテンツ情報が出力された媒体から該文書のコンテンツ情報を読み取る読取手順と、

上記文書のコンテンツ情報に埋め込まれた埋め込み情報を抽出する抽出手順と、

上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を取得する取得手順と、

上記文書属性情報を上記文書のコンテンツ情報を入出力する入出力装置へ送信する文書属性情報送信手順とを有することを特徴とする入出力装置ドライバプログラム。

【請求項１８】　上記取得手順は、上記埋め込み情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手順と、

上記管理手段から送信された上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を受信する受信手順とを有することを特徴とする請求項１７記載の入出力装置ドライバプログラム。

【請求項１９】　文書を処理する文書処理手段との間で該文書のセキュリティに関する情報が格納された文書ファイルの送受信を制御するドキュメントセキュリティプロファイル方法であって、

第１の文書処理手段から上記文書ファイルを受信する第１の受信手順と、

上記文書に関する処理の要件を有するセキュリティポリシーに基づいて、上記文書ファイルに対応する上記文書のセキュリティに関する文書属性情報を付加して上記第１の文書処理手段に送信する第１の送信手順とを有することを特徴とするドキュメントセキュリティプロファイル方法。

【請求項２０】　第２の文書処理手段から上記文書に関する処理を行うユーザーを識別するユーザー属性情報を受信する第２の受信手順と、

上記ユーザー属性情報に基づいて、上記文書の処理の可否を上記第２の文書処理手段に送信する第２の送信手順とを有することを特徴とする請求項１９記載のドキュメントセキュリティプロファイル方法。

【請求項２１】　上記第１の送信手順は、上記文書ファイルに、上記文書属性情報、上記ユーザー属性情報、及び上記文書に関する処理を許可する要件、上記文書に関する処理を禁止する要件、上記セキュリティポリシーのうち少なくとも一つを付加して上記第１の入出力装置に送信することを特徴とする請求項１９又は２０記載のドキュメントセキュリティプロファイル方法。

【請求項２２】　文書のセキュリティに関する情報が格納された文書ファイルの配布を行うドキュメントセキュリティプロファイル方法であって、

上記文書ファイルを上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する第１の送信手順と、

上記管理手段から上記文書に関する処理の要件が付加された文書ファイルを受信する第１の受信手順と、

上記文書に関する処理の要件が付加された文書ファイルを上記文書を処理する他の文書処理手段に送信する文書ファイル送信手順とを有することを特徴とするドキュメントセキュリティプロファイル方法。

【請求項２３】　上記文書に関する処理の要件が付加された文書ファイルを受信する第２の受信手順と、

上記文書に関する処理の要件及び上記文書に関する処理結果に基づいて、上記文書に関する処理を行うユーザーを識別する識別手順と、

上記識別手順の識別結果を示すユーザー属性情報に対応する上記文書の処理の可否を取得する取得手順と、

上記ユーザー属性情報及び上記文書の処理の可否に基づいて、上記文書のコンテンツ情報を入出力する入出力手段を制御する制御手順とを有することを特徴とする請求項２２記載のドキュメントセキュリティプロファイル方法。

【請求項２４】　上記第１の受信手順は、上記文書ファイルに、上記文書属性情報、上記ユーザー属性情報、及び上記文書に関する処理を許可する要件、上記文書に関する処理を禁止する要件、上記セキュリティポリシーのうち少なくとも一つを付加することを特徴とする請求項２２又は２３記載のドキュメントセキュリティプロファイル方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ドキュメントセキュリティプロファイル方法に係り、特に、ドキュメント（文書）に関するセキュリティ情報を送受信するドキュメントセキュリティプロファイル方法に関する。

【０００２】

また、本発明は、そのようなドキュメントセキュリティプロファイル方法における処理を行う入出力装置、入出力装置アダプタ、入出力装置ドライバプログラムに関する。

【０００３】

【従来の技術】

近年、多くのオフィス業務では、プリンタ、複合機などの入出力装置を用いて文書が扱われている。このような入出力装置に依存して日常の業務が行われるにつれて、その文書を扱う入出力装置のセキュリティ確保が重要視されるようになってきている。特に、最近では官公庁を中心としてＩＳＯ１７７９９として知られる情報セキュリティ管理標準に基づいて組織の情報セキュリティを掲げるところが増え、そのポリシーに基づいてセキュリティを確保した入出力装置に関するシステムの構築・運営が行われている。このような動向は、官公庁から自治体、そして取引先である大手企業に広がる傾向にあり、大手企業の取引先である中小企業へとその動きが広がっていくことが容易に予想できる。この動向そのものは、健全な入出力装置システムの構築を加速させるものとして歓迎すべきである。

【０００４】

また、上記のような入出力装置システムに設定するセキュリティ情報（通常ポリシーファイルという形式で設定される）には、例えば、Ｊａｖａ（登録商標）に設定するプログラムの実行許諾に関する設定情報や、ファイアウォールに設定するプロトコルの通過許可に関する設定情報などがある。

【０００５】

一般に、入出力装置システムのセキュリティの確保は、機密性、完全性、可用性の確保に大別される。完全性や可用性は入出力装置システムの管理者が適切に運営・管理すれば、実質上問題のないレベルを確保できる場合が多い。一方、機密性の確保のためには、中小企業に代表される入出力装置のユーザー組織に所属するユーザーのそれぞれにセキュリティポリシーを共有・徹底させなければならない。このような理由で、特に、入出力装置のコンテナである文書に対するポリシー、中でも機密保持に関するポリシーが重要視されているため、多くの企業では、文書に関するセキュリティを制御する要求が高まっている。

【０００６】

例えば、従来技術として、識別情報を付加して印刷処理を行い、他の機器からの識別情報の問い合わせに答える文書管理装置と他の機器が接続された文書管理システムでは、プリンタで出力するときは良いが、他の機器でその文書が取り扱われるときに、文書管理システム全体が機能している必要がある。また、他の機

器で必要となる情報が大きくない場合でも、文書管理システム全体で管理している大きな情報を検索する必要もある（例えば、特許文献１参照）。

【０００７】

また、従来技術として、特開平７－１５４６１７号（特許文献８参照）の機密文書を識別して、コピーを停止する、コピー時の情報を同時に印字する方法と、特開平７－１５４６１７号（特許文献８参照）の機密認識マークを検知して複写動作の制御を行う方法では、紙文書の特定のパターンや機密認識マークなどの情報を複写機内部に登録しておくため、それらの情報に柔軟性がなく、それに付随する動作にも柔軟性がない（例えば、特許文献２参照）。

【０００８】

また、従来技術として、画像から特定の記号を取り出し、認識する方法では、画像への出力方法まで言及されていないため、紙の出力と入力、電子ファイルの出力と入力などの連携をとることはできない（例えば、特許文献３参照）。

【０００９】

また、従来技術として、ユーザーの識別情報に関連した印刷、複写の制御はいくつか出されているが、文書の識別情報を印刷し、複写、配布し、読み出しなどの一連の動作で扱うような出願は見られない（例えば、特許文献４参照）。

【００１０】

【特許文献１】

特開２０００－２６１５８４号公報

【特許文献２】

特許第３２０３１０３号明細書

【特許文献３】

特開平７－６６９７０号公報

【特許文献４】

特開２００１－１２５７５９号公報

【特許文献５】

特開２００２－１９７１０１号公報

【特許文献６】

特開２００２－１９７１０１号公報

【特許文献７】

特開平７－５８９５０号公報

【特許文献８】

特開平７－１５４６１７号公報

【００１１】

【発明が解決しようとする課題】

上記のように現在、多くの企業ではセキュリティ情報を設定し、そのセキュリティを制御しようとしているが、実際、オフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、また、オフィスシステムを構成するさまざまな入出力装置に関して、個別にセキュリティ設定を行う必要がある。従って、このようなセキュリティ設定を行うためにさまざまな入出力装置に関する知識が必要となってしまうという問題点があった。

【００１２】

また、複数の入出力装置の一つ一つにセキュリティ情報を設定しなければならならず、手間が煩雑になるという問題点があった。

【００１３】

このように従来の複数の入出力装置では個別にセキュリティ設定を行っているため、入出力装置システム全体がどのようなセキュリティ状態になっているかを把握するのが難しいという問題点があった。

【００１４】

そこで、本発明の課題は、文書に関するセキュリティ情報を送受信して複数の入出力装置のセキュリティを統括して管理し、そのセキュリティを反映させた文書に関する処理を行うことができるドキュメントセキュリティプロファイル方法、及びその方法における処理を行う入出力装置、入出力装置アダプタ、入出力装置ドライバプログラムを提供することである。

【００１５】

【課題を解決するための手段】

上記の課題を解決するため、本発明は、入出力装置との文書のセキュリティに

関する情報の送受信を制御するドキュメントセキュリティプロファイル方法であって、第１の入出力装置から受信した文書のセキュリティに関する文書属性情報に基づいて、上記文書のコンテンツに埋め込まれる埋め込み情報を上記第１の入出力装置に送信する第１送受信手順と、第２の入出力装置から受信した上記埋め込み情報に基づいて、上記文書属性情報を上記第２の入出力装置に送信する第２送受信手順とを有する構成とされる。

【００１６】

このようなドキュメントセキュリティプロファイル方法では、第１の入出力装置から受信した文書のセキュリティに関する文書属性情報に基づいて、文書のコンテンツに埋め込まれる埋め込み情報を第１の入出力装置に送信し、第２の入出力装置から受信した埋め込み情報に基づいて、文書属性情報を第２の入出力装置に送信することにより、文書に関するセキュリティ情報を送受信して複数の入出力装置のセキュリティを統括して管理し、そのセキュリティを反映させた文書に関する処理を行うことができる。

【００１７】

文書のセキュリティに関する情報を管理するという観点から、本発明は、請求項２に記載されるように、上記文書を識別する識別情報に対応付けて上記文書属性情報と上記埋め込み情報とを文書情報として管理する文書情報管理手順を有し、上記第１送受信手順は、上記文書情報に基づいて上記埋め込み情報を上記第１の入出力装置に送信し、上記第２送受信手順は、上記文書情報に基づいて上記文書属性情報を上記第２の入出力装置に送信するように構成することができる。

【００１８】

このようなドキュメントセキュリティプロファイル方法では、文書を識別する識別情報に対応付けて文書属性情報と埋め込み情報とを文書情報として管理し、文書情報に基づいて埋め込み情報を第１の入出力装置に送信し、文書情報に基づいて文書属性情報を第２の入出力装置に送信することにより、効率的に文書情報から文書属性情報や埋め込み情報を参照して入出力装置に送信することができる。

【００１９】

文書のコンテンツへ埋め込まれる埋め込み情報を様々な情報で適応させるという観点から、本発明は、請求項３に記載されるように、上記埋め込み情報は、上記文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であるように構成することができる。

【００２０】

このようなドキュメントセキュリティプロファイル方法では、埋め込み情報が文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であることにより、埋め込み情報で文書のコンテンツや文書属性を識別することができる。

【００２１】

埋め込み情報と共に文書のコンテンツ情報を出力するという観点から、本発明は、請求項４に記載されるように、文書のコンテンツ情報を入出力する入出力装置であって、上記文書を処理する文書処理手段から上記文書のコンテンツ情報の出力を指示する指示情報を受信する指示情報受信手段と、上記指示情報に基づいて上記文書のセキュリティに関する文書属性情報を抽出する抽出手段と、上記文書属性情報に対応する上記文書のコンテンツに埋め込まれる埋め込み情報を取得する取得手段と、上記埋め込み情報と共に上記文書のコンテンツ情報を出力する出力手段とを有する構成とすることができる。

【００２２】

このような入出力装置では、文書を処理する文書処理手段から文書のコンテンツ情報の出力を指示する指示情報を受信し、指示情報に基づいて文書のセキュリティに関する文書属性情報を抽出し、文書属性情報に対応する文書のコンテンツに埋め込まれる埋め込み情報を取得し、埋め込み情報と共に文書のコンテンツ情報を出力することにより、文書に関するセキュリティ情報を取得して、そのセキュリティを反映させた文書に関する印刷処理などを行うことができる。

【００２３】

文書属性情報に対応する埋め込み情報を受信するという観点から、本発明は、請求項５に記載されるように、上記取得手段は、上記文書属性情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、

上記管理手段から送信された上記文書属性情報に対応する上記埋め込み情報を受信する受信手段とを有するように構成することができる。

【００２４】

このような入出力装置では、文書属性情報を文書のセキュリティに関するプロファイルを管理する管理手段に送信し、管理手段から送信された文書属性情報に対応する埋め込み情報を受信することにより、文書に関するセキュリティ情報を送受信して、そのセキュリティを反映させた文書に関する印刷処理などを行うことができる。

【００２５】

文書属性情報に基づいて文書に関する処理を制御するという観点から、本発明は、請求項７に記載されるように、文書のコンテンツ情報を入出力する入出力装置であって、上記文書のコンテンツ情報が出力された媒体から該文書のコンテンツ情報を読み取る読取手段と、上記文書のコンテンツ情報に埋め込まれた埋め込み情報を抽出する抽出手段と、上記埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を取得する取得手段と、上記文書属性情報に基づいて上記文書に関する処理を制御する制御手段とを有するように構成することができる。

【００２６】

このような入出力装置では、上記文書のコンテンツ情報が出力された媒体から該文書のコンテンツ情報を読み取り、文書のコンテンツ情報に埋め込まれた埋め込み情報を抽出し、埋め込み情報に対応する文書のセキュリティに関する文書属性情報を取得し、文書属性情報に基づいて文書に関する処理を制御することにより、文書に関するセキュリティ情報を取得して、そのセキュリティを反映させた文書に関する処理を制御することができる。

【００２７】

埋め込み情報に対応する文書属性情報を受信するという観点から、本発明は、請求項８に記載されるように、上記取得手段は、上記埋め込み情報を上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する送信手段と、上記管理手段から送信された上記埋め込み情報に対応する上記文書のセキュリテ

ィに関する文書属性情報を受信する受信手段とを有するように構成することができる。

【００２８】

このような入出力装置では、埋め込み情報を文書のセキュリティに関するプロファイルを管理する管理手段に送信し、管理手段から送信された埋め込み情報に対応する上記文書のセキュリティに関する文書属性情報を受信することにより、文書に関するセキュリティ情報を送受信して、そのセキュリティを反映させた文書に関する印刷処理などを行うことができる。

【００２９】

文書のセキュリティに関する情報を管理するという観点から、本発明は、請求項９に記載されるように、上記文書を識別する識別情報に対応付けて上記文書属性情報と上記埋め込み情報とを文書情報として管理する文書情報管理手段を有するように構成することができる。

【００３０】

このような入出力装置では、文書を識別する識別情報に対応付けて文書属性情報と埋め込み情報とを文書情報として管理することにより、効率的に文書属性情報を取得して、そのセキュリティを反映させた文書に関する印刷処理などを行うことができる。

【００３１】

セキュリティポリシーに基づいた情報を付加した文書ファイルを送受信するという観点から、本発明は、請求項１９に記載されるように、文書を処理する文書処理手段との間で該文書のセキュリティに関する情報が格納された文書ファイルの送受信を制御するドキュメントセキュリティプロファイル方法であって、第１の文書処理手段から上記文書ファイルを受信する第１の受信手順と、上記文書に関する処理の要件を有するセキュリティポリシーに基づいて、上記文書ファイルに対応する上記文書のセキュリティに関する文書属性情報を付加して上記第１の文書処理手段に送信する第１の送信手順とを有するように構成することができる。

【００３２】

このようなドキュメントセキュリティプロファイル方法では、第１の文書処理手段から上記文書ファイルを受信し、文書に関する処理の要件を有するセキュリティポリシーに基づいて、文書ファイルに対応する文書のセキュリティに関する文書属性情報を付加して第１の文書処理手段に送信することにより、文書を処理する文書処理手段との間でセキュリティを反映させた文書ファイルの送受信を制御することができる。

【００３３】

セキュリティポリシーに基づいた情報を付加した文書ファイルを送受信するという観点から、本発明は、請求項２０に記載されるように、第２の文書処理手段から上記文書に関する処理を行うユーザーを識別するユーザー属性情報を受信する第２の受信手順と、上記ユーザー属性情報に基づいて、上記文書の処理の可否を上記第２の文書処理手段に送信する第２の送信手順とを有するように構成することができる。

【００３４】

このようなドキュメントセキュリティプロファイル方法では、第２の文書処理手段から文書に関する処理を行うユーザーを識別するユーザー属性情報を受信する第２の受信手順と、ユーザー属性情報に基づいて、文書の処理の可否を第２の文書処理手段に送信することにより、セキュリティポリシーに基づいて複数の文書処理手段での処理を制御することができる。

【００３５】

文書のセキュリティに関する情報に柔軟性を持たせるという観点から、本発明は、請求項２１に記載されるように、上記第１の送信手順は、上記文書ファイルに、上記文書属性情報、上記ユーザー属性情報、及び上記文書に関する処理を許可する要件、上記文書に関する処理を禁止する要件、上記セキュリティポリシーのうち少なくとも一つを付加して上記第１の入出力装置に送信するように構成することができる。

【００３６】

このようなドキュメントセキュリティプロファイル方法では、文書ファイルに、文書属性情報、ユーザー属性情報、文書に関する処理を許可する要件、文書に

関する処理を禁止する要件、セキュリティポリシーのうち少なくとも一つを付加することにより、効率的に複数の文書処理手段での処理を制御することができる。

【００３７】

文書処理手段により文書のセキュリティに関する情報が格納された文書ファイルの配布を行うという観点から、本発明は、請求項２２に記載されるように、文書のセキュリティに関する情報が格納された文書ファイルの配布を行うドキュメントセキュリティプロファイル方法であって、上記文書ファイルを上記文書のセキュリティに関するプロファイルを管理する管理手段に送信する第１の送信手順と、上記管理手段から上記文書に関する処理の要件が付加された文書ファイルを受信する第１の受信手順と、上記文書に関する処理の要件が付加された文書ファイルを上記文書を処理する他の文書処理手段に送信する文書ファイル送信手順とを有するように構成することができる。

【００３８】

このようなドキュメントセキュリティプロファイル方法では、文書ファイルを文書のセキュリティに関するプロファイルを管理する管理手段に送信し、管理手段から上記文書に関する処理の要件が付加された文書ファイルを受信し、文書に関する処理の要件が付加された文書ファイルを、その文書を処理する他の文書処理手段に送信することにより、文書処理手段により文書のセキュリティに関する情報が付加された文書ファイルを受信し、受信した文書ファイルを他の文書処理手段に配布することができる。

【００３９】

セキュリティポリシーに基づいた情報を付加した文書ファイルを送受信するという観点から、本発明は、請求項２３に記載されるように、上記文書に関する処理の要件が付加された文書ファイルを受信する第２の受信手順と、上記文書に関する処理の要件及び上記文書に関する処理結果に基づいて、上記文書に関する処理を行うユーザーを識別する識別手順と、上記識別手順の識別結果を示すユーザー属性情報に対応する上記文書の処理の可否を取得する取得手順と、上記ユーザー属性情報及び上記文書の処理の可否に基づいて、上記文書の処理を行う処理手

順とを有するように構成することができる。

【００４０】

このようなドキュメントセキュリティプロファイル方法では、文書に関する処理の要件が付加された文書ファイルを受信し、文書に関する処理の要件及び文書に関する処理結果に基づいて、文書に関する処理を行うユーザーを識別し、識別手順の識別結果を示すユーザー属性情報に対応する文書の処理の可否を取得し、ユーザー属性情報及び文書の処理の可否に基づいて、文書のコンテンツ情報を入出力する入出力手段を制御することにより、配布された文書ファイルに基づいて、効率的に入出力手段の処理を制御することができる。

【００４１】

また、上記課題を解決するため、本発明は、上記ドキュメントセキュリティプロファイル方法における処理を行う入出力装置アダプタ、入出力装置ドライバプログラムとすることもできる。

【００４２】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。本発明の実施の一形態に係るドキュメントセキュリティプロファイル方法は、プリンタや複合機などの入出力装置へ文書属性情報や埋め込み情報を送受信する。その入出力装置のハードウェア構成は、例えば、図１に示すようになっている。尚、上記プロファイルとは、文書のセキュリティに関する情報を示している。

【００４３】

図１は、本発明の第１実施例に係る入出力装置のハードウェア構成を示すブロック図である。

【００４４】

図１において、入出力装置１０は、ＣＰＵ１１と、ＲＯＭ１２と、ＲＡＭ１３と、ＨＤＤ１４と、スキャナ１５と、プロッタ１６と、表示操作部１７と、ＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）１８とで構成される。これらの各ユニットはバス１９を介して接続されている。ＣＰＵ１１は、ＲＯＭ１２に格納された入出力装置を制御するためのプログラム（ドライバプログラム）

、及びＨＤＤ１４からＲＡＭ１３に転送されるプログラムとに基づいて、入出力装置１０を制御する。また、ＣＰＵ１１は、ＲＡＭ１３を作業メモリ空間として利用すると共に、ＲＡＭ１３から処理対象のデータを読み出して処理する。処理後のデータはＲＡＭ１３に格納される。ＨＤＤ１４は、文書ファイル、ドキュメントセキュリティプロファイル方法に係るプログラムなどを格納する。スキャナ１５は、印刷物をスキャンして電子データとして取り込むスキャナ処理を行う。プロッタ１６は、パーソナルコンピュータ（ＰＣ）などで生成した電子文書を印刷する場合や、印刷物などを複写する印刷処理を行う。ＮＩＣ１８は、ネットワークインターフェースであり、ネットワークと接続されて複数の入出力装置とドキュメントセキュリティプロファイル方法に関する文書属性、埋め込み情報などの送受信を行う。表示操作部１７は、オペレーションパネルなどで構成され、ユーザーからの入力操作の受け付け並びにユーザーに向けた表示を行う。

【００４５】

このようなハードウェア構成を採用することにより、複数の入出力装置１０のセキュリティを統括して管理し、そのセキュリティを反映させた印刷処理などを行うことができる。

【００４６】

次に、第１実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図２は、本発明の第１実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。図２において、ドキュメントセキュリティシステム２は、文書に関する処理を制御する文書処理部２０と、ドキュメントセキュリティプロファイル方法における処理が行われるドキュメントセキュリティプロファイル処理部３０と、図２に示す入力装置１０の構成を有するプリンタ４０、複合機５０とで構成される。尚、文書処理部２０と、ドキュメントセキュリティプロファイル処理部３０と、プリンタ４０と、複合機５０は、ＬＡＮなどのネットワーク１を介して接続されている。尚、文書処理部２０と、ドキュメントセキュリティプロファイル処理部３０は、それぞれ別のサーバに設置するようにしてもよいし、一つのサーバに設置するようにしてもよい。

【００４７】

文書処理部２０は、プリンタ４０に文書のプリントを指示する情報を送信する。ドキュメントセキュリティプロファイル処理部３０は、プリンタ４０及び複合機５０へ文書に関するセキュリティ情報を送受信する。プリンタ４０は、例えば、文書情報及び文書に関するセキュリティ情報を紙へプリントする出力処理を行う。複合機５０は、例えば、紙にプリントされた文書情報及び文書に関するセキュリティ情報をスキャンする入力処理を行う。

【００４８】

次に、第１実施例におけるドキュメントセキュリティプロファイル処理の手順について説明する。図２に示すように、先ず、ステップＳ１の処理で、文書処理部２０は、プリンタ４０に文書のプリントを指示する指示情報を送信する。この指示情報には、プリントする文書情報、文書属性を含んでいる。ステップＳ２の処理で、プリンタ４０は、指示情報から文書属性を抽出し、その文書属性をドキュメントセキュリティプロファイル処理部３０に送信する。ステップＳ３の処理で、ドキュメントセキュリティプロファイル処理部３０は、送信された文書属性に基づいて、文書情報への埋め込み情報を作成し、プリンタ４０に送信する。ステップＳ４の処理で、プリンタ４０は、受信した埋め込み情報に基づいて、紙６０に文書情報と共に埋め込み情報６１をプリントする出力処理を行う。

【００４９】

ステップＳ５の処理で、複合機５０は、紙６０にプリントされた文書情報と共に埋め込み情報６１をスキャンする入力処理を行う。ステップＳ６の処理で、複合機６０は、ドキュメントセキュリティプロファイル処理部３０にスキャンした埋め込み情報６１を送信する。ステップＳ７の処理で、ドキュメントセキュリティプロファイル処理部３０は、埋め込み情報６１に基づいて文書属性を取得し、その文書属性を複合機５０に送信する。複合機５０は、受信した文書属性に基づいてスキャンした文書情報に関する処理を制御する。複合機５０の処理について、例えば、複写処理の場合、複写の停止や、「複写禁止」、「社外秘」などのラベルを印字する、ユーザー情報、日時情報を印字する、特殊な紙への複写、複写の履歴情報の格納などの処理を行う。また、複合機５０は、スキャンした文書に

関する情報の配信処理の場合、配信の停止、「複写禁止」、「社外秘」などのすかしを追加する、ユーザー情報、日時情報を追加する、特定のフォルダへのコピー配信、配信の履歴情報の格納などの処理を行う。

【００５０】

次に、第２実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図３は、本発明の第２実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。尚、図３に示すシステム構成は、図２に示すシステム構成と略同様であるため、同様の構成及び手順については同符号を付し、また、同様の構成のうち一部分の構成を省略する。以下、図５、図６、図８に示すシステム構成についても同様とする。

【００５１】

図３において、ドキュメントセキュリティシステム３は、文書属性と埋め込み情報である画像情報とが格納された文書情報ＤＢ３１を有する構成とされる。ドキュメントセキュリティプロファイル処理部３０は、送信された文書属性に基づいて、文書情報ＤＢ３１に格納された埋め込み情報６１をプリンタ４０に送信する。プリンタ４０は、送信された埋め込み情報６１に基づいて、紙６０に文書情報に重ねて埋め込み情報６１をプリントする。

【００５２】

次に、文書情報ＤＢ３１に格納された文書情報について説明する。図４は、文書情報ＤＢに格納されたテーブルを示す図である。図４において、テーブル３１０は、文書を識別する文書ＩＤと、文書属性を格納した文書属性ファイルと、埋め込み情報とで構成される。ここで文書ＩＤは、日時やドキュメントセキュリティプロファイル処理部３０を識別するＩＤや、プリンタ４０を識別するＩＤなどの組み合わせ、また、それにシリアル番号などを付加して一意に定まる情報が用いられている。尚、埋め込み情報は、文書を一意に識別するバーコード情報、透かし情報、地紋情報などが適応される。例えば、バーコード情報の場合、文書ＩＤをそのままエンコードしたり、シリアル番号などをエンコードしたりして一意に定まる情報を格納している。尚、テーブル３１０に格納される情報は、文書の保存期限などが定められている場合、その保存期限内は唯一のＩＤとなるように

設定する。

【００５３】

次に、第３実施例におけるドキュメントセキュリティプロファイル処理部３０が複合機５１内に設けられた場合のシステム構成について説明する。図５は、本発明の第３実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。図５において、ドキュメントセキュリティシステム４は、文書属性と埋め込み情報である画像情報とが格納された文書情報ＤＢ３１と、ドキュメントセキュリティプロファイル処理部３０が設けられた複合機５１とを有する構成とされる。このように、複合機５１内にドキュメントセキュリティプロファイル処理部３０を設置することにより、他のサーバを設置して動作させる必要がないため、システムの簡略化を図ることができる。

【００５４】

次に、第４実施例におけるプリンタが除かれた場合のシステム構成について説明する。図６は、本発明の第４実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。図６において、ドキュメントセキュリティシステム５は、文書属性と埋め込み情報である画像情報とが格納された文書情報ＤＢ３１と、プリント機能を有し、ドキュメントセキュリティプロファイル処理部３０が設けられた複合機５１とを有する構成とされる。先ず、複合機５１は、文書処理部２０からのプリント指示情報を受信すると、ステップＳ２の処理で、複合機５１のドキュメントセキュリティプロファイル処理部３０は、文書情報ＤＢ３１から文書属性を参照する。また、ステップＳ３の処理で、ドキュメントセキュリティプロファイル処理部３０は、文書情報ＤＢ.３１から埋め込み情報６１を受信する。このように、プリンタ４０を除き、複合機５１内にドキュメントセキュリティプロファイル処理部３０を設置することにより、他のサーバを設置して動作させる必要がないため、システムの簡略化を図ることができる。

【００５５】

次に、第５実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図７は、本発明の第５実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。尚、図７に示す

システム構成は、図２に示すシステム構成と略同様であるため、同様の構成及び手順については同符号を付して説明を省略する。図７において、ドキュメントセキュリティシステム６は、ドキュメントセキュリティプロファイル処理部３０からの文書に関する情報の送受信をプリンタ４０、複合機５０が対応することができない場合、プリンタ４０に接続されたアダプタ７０と、複合機５０に接続されたアダプタ７１とを有する構成とされる。

【００５６】

次に、各アダプタ７０、７１での処理手順を説明する。先ず、ステップＳ１の処理で、プリンタ４０に接続されたアダプタ７０は、文書処理部２０から文書のプリントを指示する指示情報を受信する。ステップＳ２の処理で、アダプタ７０は、ドキュメントセキュリティプロファイル処理部３０へ文書属性を送信する。ステップＳ３の処理で、アダプタ７０は、ドキュメントセキュリティプロファイル処理部３０からの埋め込み情報を受信する。ステップＳ４の処理で、プリンタ４０は、アダプタ７０から取得した埋め込み情報に基づいて、紙６０に文書情報と共に埋め込み情報６１をプリントする出力処理を行う。

【００５７】

一方、ステップＳ５の処理で、複合機５０は、紙６０にプリントされた文書情報と共に埋め込み情報６１をスキャンする入力処理を行う。ステップＳ６の処理で、アダプタ７１は、ドキュメントセキュリティプロファイル処理部３０へ埋め込み情報を送信する。ステップＳ７の処理で、アダプタ７１は、ドキュメントセキュリティプロファイル処理部３０からの文書属性を受信する。複合機５０は、受信した文書属性に基づいてスキャンした文書情報に関する処理を制御する。

【００５８】

このように、プリンタ４０に接続されたアダプタ７０と、複合機５０に接続されたアダプタ７１とを設けることにより、ドキュメントセキュリティプロファイル処理部３０からの文書に関する情報の送受信を行うことができる。

【００５９】

次に、第６実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図８は、本発明の第６実施例に係るドキュメント

セキュリティプロファイル方法におけるシステム構成図である。図８において、ドキュメントセキュリティシステム７は、文書のプリント指示情報を送信する前に、ドキュメントセキュリティプロファイル処理部３０から埋め込み情報を取得する文書処理部２０を有する構成とされる。先ず、ステップＳ１の処理で、文書処理部２０は、ドキュメントセキュリティプロファイル処理部３０へ文書属性を送信する。ステップＳ２の処理で、ドキュメントセキュリティプロファイル処理部３０は、受信した文書情報に基づいて、文書処理部２０へ埋め込み情報を送信する。ステップＳ３の処理で、文書処理部２０は、プリンタ４０へ埋め込み情報と共に、効率的にプリントを指示する指示情報を送信する。

【００６０】

このように、文書処理部２０はプリンタ４０へ埋め込み情報と共に、プリントを指示する指示情報を送信することにより、プリンタ４０で文書情報のプリントを行う出力処理を効率的に行うことができる。

【００６１】

尚、プリンタ４０に送信される埋め込み情報に、複合機５０を制御する情報を付加するようにしてもよい。これにより、ドキュメントセキュリティプロファイル処理部３０が停止している場合、複合機５０での処理を制御することができる。例えば、複合機５０で「極秘」などの文書属性が抽出された場合、複写処理を停止するなどの基本的な制御情報を付加することができる。

【００６２】

尚、プリンタ４０又は複合機５０で文書に関する入出力処理を行うときに、ドキュメントセキュリティプロファイル処理部３０が停止している場合、文書属性を抽出し、即座に動作を停止することなく、最小限の情報で最低限の入出力処理を行う第一の埋め込み情報と、より多くの文書に関する情報を抽出して様々な処理を制御するための第二の埋め込み情報とを埋め込むようにしてもよい。

【００６３】

次に、電子的な埋め込み情報としてＰＤＦ（Ｐｏｒｔａｂｌｅ　Ｄｏｃｕｍｅｎｔ　Ｆｏｒｍａｔ）ファイルを用い、ドキュメントセキュリティポリシー（以下総称してＤＳＰ（Ｄｏｃｕｍｅｎｔ　Ｓｅｃｕｒｉｔｙ　Ｐｏｌｉｃｙ）と呼

ぶ）に基づいて文書に関する情報を送受信する第７実施例に説明する。

【００６４】

先ず、第７実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図９は、本発明の第７実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。図９において、ドキュメントセキュリティシステム８は、ＰＤＦ２００を有するドキュメントセキュリティプロファイル処理部３２と、文書属性とＰＤＦファイルを送受信する文書処理部２１と、ユーザーを認証するプラグインを有する文書処理部２２とを有する構成とされる。

【００６５】

次に、ドキュメントセキュリティシステム８での処理手順を説明する。先ず、ステップＳ１の処理で、文書処理部２１は、ドキュメントセキュリティプロファイル処理部３２に文書属性と、ＰＤＦファイル２５とを送信する。ステップＳ２の処理で、ドキュメントセキュリティプロファイル処理部３２は、文書情報をＰＤＦファイル２５に埋め込み、セキュリティプロテクトされたＰＤＦファイル２６を文書処理部２１に送信する。ステップＳ３の処理で、文書処理部２１は、受信したセキュリティプロテクトされたＰＤＦファイル２６を文書処理部２２に配布する。

【００６６】

ステップＳ４の処理で、文書処理部２２は、配布されたＰＤＦファイル２６に基づいて文書の読み取り、印刷などの処理（イベント）を行う。ステップＳ５の処理で、文書処理部２２のプラグイン３５では、ＰＤＦファイル２６を受信すると、ユーザーの認証が自動的に起動する。ステップＳ６の処理で、プラグイン３５は、ＰＤＦファイル２５に埋め込まれた文書属性と、ユーザー認証により取得したユーザー属性と、イベントとをドキュメントセキュリティプロファイル処理部３２に送信する。ステップＳ７の処理で、ドキュメントセキュリティプロファイル処理部３２は、受信した文書属性、ユーザー属性、イベントとをＤＳＰ２００に基づいて、その文書に関する処理の許可、禁止、許可の場合の要件等を判断する。ステップＳ８の処理で、ドキュメントセキュリティプロファイル処理部３

２は、文書に関する処理の許可、禁止、許可の場合の要件等の判断結果を文書処理部２２に送信する。

【００６７】

このように、ＰＤＦファイル２５、２６及びＤＳＰ２００に基づいて、文書の読み取り、印刷などの処理を制御する情報を送受信することにより、文書のセキュリティの機密性を確保することができ、文書に関するセキュリティを統括して管理することができる。

【００６８】

尚、埋め込み情報を埋め込んだＰＤＦファイル２５、２６には、埋め込み情報を抽出するためのプログラム（例えば、ＡｃｒｏｂａｔのＰｌｕｇ－ｉｎモジュール）がないと開けないように設定された情報を付加するようにしてもよい。

【００６９】

次に、第８実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図１０は、本発明の第８実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。尚、図１０に示すシステム構成は、図９に示すシステム構成と略同様であるため、同様の構成及び手順については同符号を付して説明を省略する。以下、図１１に示すシステム構成についても同様とする。図１０において、ドキュメントセキュリティシステム８０は、文書処理部２１でＰＤＦファイル２５を作成する時に、ＤＳＰ２００に基づいて文書に関する処理の許可、禁止、許可の場合の要件等の判断を行うドキュメントセキュリティプロファイル処理部３２を有する構成とされる。

【００７０】

次に、ドキュメントセキュリティシステム８０での処理手順を説明する。先ず、ステップＳ１の処理で、文書処理部２１は、ドキュメントセキュリティプロファイル処理部３２に文書属性と、ユーザー属性と、ＰＤＦファイル２５とを送信する。ステップＳ２の処理で、ドキュメントセキュリティプロファイル処理部３２は、受信した文書属性、ユーザー属性をＤＳＰ２００に基づいて、その文書に関する処理の許可、禁止、許可の場合の要件等を判断する。ステップＳ３の処理で、ドキュメントセキュリティプロファイル処理部３２は、文書に関する処理の

許可、禁止、許可の場合の要件等の判断結果をＰＤＦファイル２５に埋め込み、セキュリティプロテクトされたＰＤＦファイル２６を文書処理部２１に送信する。ステップＳ４の処理で、文書処理部２１は、受信したセキュリティプロテクトされたＰＤＦファイル2.6を文書処理部２２に配布する。

【００７１】

ステップＳ５の処理で、文書処理部２２は、配布されたＰＤＦファイル２６に基づいて文書の読み取り、印刷などの処理（イベント）を行う。ステップＳ６の処理で、文書処理部２２のプラグイン３５では、ＰＤＦファイル２６を受信すると、ユーザーの認証が自動的に起動される。ステップＳ７の処理で、プラグイン３５は、ＰＤＦファイル２６に埋め込まれたユーザー属性、イベントに対する判断結果に基づいて処理を行う。

【００７２】

このように、文書処理部２２は、文書処理部２１でＰＤＦファイル２５を作成する時に、ＤＳＰ２００に基づいて判断された判断結果と文書の読み取り、印刷などの処理を制御する情報を送受信することにより、文書のセキュリティの機密性を確保することができ、効率的に文書に関するセキュリティを統括して管理することができる。

【００７３】

次に、第９実施例におけるドキュメントセキュリティプロファイル方法でのシステム構成について説明する。図１１は、本発明の第９実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。図１１において、ドキュメントセキュリティシステム８００は、文書処理部２１でＰＤＦファイル２５を作成する時に、そのＰＤＦファイル２５にＤＳＰ２００を埋め込み、ＤＳＰ２００に基づいて文書に関する処理の許可、禁止、許可の場合の要件等の判断を行うプラグイン３５を有する構成とされる。

【００７４】

次に、ドキュメントセキュリティシステム８００での処理手順を説明する。先ず、ステップＳ１の処理で、文書処理部２１は、ドキュメントセキュリティプロファイル処理部３２に文書属性と、ＰＤＦファイル２５とを送信する。ステップ

Ｓ２の処理で、ドキュメントセキュリティプロファイル処理部３２は、文書情報をＰＤＦファイル２５に埋め込み、セキュリティプロテクトされたＰＤＦファイル２６を文書処理部２１に送信する。ステップＳ３の処理で、文書処理部２１は、受信したセキュリティプロテクトされたＰＤＦファイル２６を文書処理部２２に配布する。

【００７５】

ステップＳ４の処理で、文書処理部２２は、配布されたＰＤＦファイル２６に基づいて文書の読み取り、印刷などの処理（イベント）を行う。ステップＳ５の処理で、文書処理部２２のプラグイン３５では、ＰＤＦファイル２６を受信すると、ユーザーの認証が自動的に起動する。ステップＳ６の処理で、プラグイン３５は、ＰＤＦファイル２５に埋め込まれた文書属性、ユーザー属性、イベントとＤＳＰ２００とに基づいて、その文書に関する処理の許可、禁止、許可の場合の要件等を判断する。ステップＳ７の処理で、プラグイン３５は、受信した文書属性、ユーザー属性、イベントとをＤＳＰ２００に基づいて、その文書に関する処理の許可、禁止、許可の場合の要件等を判断する。

【００７６】

このように、プラグイン３５がＰＤＦファイル２５、２６に埋め込まれたＤＳＰ２００に基づいて、文書の読み取り、印刷などの処理を制御する情報を送受信することにより、文書のセキュリティの機密性を確保することができ、文書に関するセキュリティを統括して管理することができる。

【００７７】

次に、ＤＳＰ２００を記述するためのセキュリティポリシーについて説明する。図１２は、ドキュメントに対するセキュリティポリシーの例を示す図である。図１２に示すセキュリティポリシー２０１は、上記入出力装置１０で取り扱うドキュメントに対して、入出力装置１０の管理者により設定されるものとする。セキュリティポリシー２０１には、極秘文書についての記述２０２と、丸秘文書についての記述２０３と、社外秘文書についての記述２０４と、人事関連文書についての記述２０５とが記述されている。各記述２０２～２０５には、各ドキュメントの複写の許可の要件と、プリントの許可の要件と、閲覧の許可の要件が設定

されている。各記述２０２～２０５に従ってドキュメントのセキュリティレベルを分類した定義ファイルに基づいてドキュメントセキュリティポリシー２００を記述する。

【００７８】

次に、ＤＳＰ２００の先頭に記述される識別情報について説明する。図１３は、ＤＳＰの識別情報を示す図である。図１３に示すＤＳＰ２００の識別情報２１０において、＜about_this_policy＞と＜/about_this_policy＞とで囲まれた範囲の記述２１１～２１３には、ＤＳＰ２００を識別するための識別情報が記述されている。記述２１１には、ＤＳＰ２００を他のＤＳＰと区別するためのシリアル番号が記述されている。記述２１２には、ＤＳＰ２００に対応する定義ファイルのシリアル番号が記述されている。尚、この定義ファイルは更新される可能性があるため、このＤＳＰ２００がどの定義ファイルに基づいて記述されているのかを明確にするために、記述２１２が記述される。記述２１３には、ＤＳＰ２００のタイトル、バージョン番号、作成日時、作成者、説明などの一般的な書誌情報が記述される。

【００７９】

以下に、ＤＳＰ２００の識別情報の後に記述される記述内容について説明する。図１４は、ＤＳＰの記述例を示す図である。図１４に示すＤＳＰ２００の記述２２０において、＜policy＞と＜/policy＞とで囲まれた範囲の記述２２１～２３１には、ドキュメントに関する情報が記述されている。記述２２０は、記述２２１に示す複数のアクセス制御ルール＜ace_rule＞で構成される。１つの記述２２１のアクセス制御ルール＜ace_rule＞は、記述２２２に示す対象のドキュメントのカテゴリ＜doc_category＞とレベル＜doc_security_level＞とが一意に設定され、記述２２３に示すアクセス制御リスト＜acl＞を１つ含むように設定される。記述２２３のアクセス制御リスト＜acl＞は、記述２２４に示す複数のアクセス制御エレメント＜ace＞で構成される。記述２２４のアクセス制御エレメント＜ace＞は、記述２２５に示すユーザーのカテゴリ＜user_category＞と、記述２２６に示すユーザーのレベル＜user_security_level＞とがセキュリティ属性として一意に設定される。さらに、記述２２４のアクセス制御エレメント＜ace

＞は、記述２２７に示す複数のオペレーション＜operation＞で構成される。

【００８０】

記述２２５に示すユーザーのカテゴリ＜user_category＞には、ユーザーに関するカテゴリが記述されている。また、記述２２６に示すユーザーのレベル＜user_security_level＞には、ユーザーに対してドキュメントのオペレーションが可能か否かを示す権限レベルが記述されている。尚、ユーザーのセキュリティ属性であるカテゴリとレベルの組み合わせを複数設定可能にすることにより、例えば、所定のユーザーが部門Ａの「丸秘」のドキュメントとプロジェクトＢの「極秘」のドキュメントの両方にアクセスすることができる。従って、ユーザーのセキュリティ属性を設けることにより、効率的にドキュメントのオペレーションを行うことができる。

【００８１】

記述２２７の各オペレーション＜operation＞には、記述２２８に示す１つのオペレーション名＜name＞と、記述２２９に示す１つの禁止＜denied/＞と、記述２３０に示す複数の＜requirement＞と、記述２３１に示す１つの許可＜allowed＞などで構成される。また、図１４に示すように、記述２２２のドキュメントのカテゴリ＜doc_category＞や、記述２２６に示すユーザーのレベル＜user_security_level＞に記述される「ＡＮＹ」は、どのカテゴリ、レベルにも適用されることを示している。また、記述２２５のユーザーのカテゴリ＜user_category＞の「ＤＯＣ＿ＣＡＴＥＧＯＲＹ」はユーザーのカテゴリがドキュメントのカテゴリと同じ場合に適用される。

【００８２】

このような構成でＤＳＰ２００を記述することにより、ドキュメントのタイプ（カテゴリ、レベル）に応じて、どのようなユーザータイプ（カテゴリ、レベル）がドキュメントに対してどのようなオペレーションが可能なのか、オペレーションが可能な場合にはどのような要件を満たさなければならないのかを明確に記述することができる。

【００８３】

また、上記ＤＳＰ２００は、プラットホームに依存しないＸＭＬ（ｅＸｔｅｎ

ｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）形式で記述することにより、各入出力装置間でのセキュリティポリシーを共有させることができる。

【００８４】

尚、セキュリティポリシーを適応させる対象は、電子的なドキュメントに限らず、上記の記述２２７のオペレーション＜operation＞に紙のドキュメントに関するオペレーション（hardcopy、scanなど）を設定することにより、紙のドキュメントに対してセキュリティポリシーを適応させることができる。

【００８５】

尚、上記の記述２２０では、禁止するオペレーションには記述２２９に示すように禁止＜denied/＞を記述しているが、ＤＳＰ２００に記述されていなければアクセスは許可されていないことを表わすようにしてもよい。

【００８６】

以下に、ＤＳＰ２００の識別情報の後に記述される記述内容の他の例について説明する。図１５は、ＤＳＰの記述例を示す図である。図１５に示すＤＳＰ２００の記述２４０において、＜policy＞と＜/policy＞とで囲まれた範囲のうち記述２４１～２４３には、ドキュメントのオペレーション許可に関する情報が記述されている。記述２４１は、＜denied_operations＞により許可しないオペレーションを列挙している。記述２４２に示す＜requirement＞explicit_authorization＜/requirement＞は、ドキュメントの管理者により明示的な許可が得られた場合に、そのオペレーションを許可する記述である。記述２４３は、＜allowed_operations＞により無条件で許可するオペレーションを列挙している。

【００８７】

このように、ＤＳＰ２００にオペレーションを明示的に許可する記述を設けることで、柔軟なオペレーション制御を行うことが可能となる。また、明示的な許可を指定可能にすることで、明示的な許可が得られれば実行可能なオペレーションと、明示的な許可が得られたとしても禁止しなければならないオペレーションとを区別することができる。

【００８８】

また、ＤＳＰ２００にオペレーション許可に関する情報を記述しないか、又は

禁止<denied/>で指定されたオペレーションは、明示的な許可が得られたとしても禁止しなければならないオペレーションとなる。これにより、ポリシーを記述している管理者側の意図が的確に設定することができ、誤って許可を与えてしまったオペレーションが実行されるというような事態を予め防ぐように設定することができる。

【００８９】

次に、ＤＳＰ２００を記述し、管理するシステム構成について説明する。図１６は、ドキュメントセキュリティポリシーの記述に関するシステム構成図である。図１６において、ドキュメントセキュリティプロファイル方法において用いられるＤＳＰ２００を記述し、管理するセキュリティ管理システム１００は、ＤＳＰの記述、記録媒体１０２への格納、ＤＳＰを以下に示すサブシステムへ伝送するセキュリティサーバー１０１と、入出力装置１０とで構成される。複数のプリンタ４０、複合機５０のそれぞれが入出力装置１０として、ネットワーク１を介してセキュリティサーバー１０１に接続される。図１６において、セキュリティサーバー２０はサーバコンピュータであって、ＣＰＵ（中央処理装置）によって各構成が制御される。ＣＰＵは、メモリユニットに格納されたプログラムに従ってセキュリティポリシー記述処理を行う。

【００９０】

以下に、セキュリティ管理システム１００でのＤＳＰに関する処理を説明する。セキュリティサーバー１０１では、セキュリティサーバー１０１の管理者によりＤＳＰ２００が記述される（ステップＳ１）。例えば、ＤＳＰ２００は、プラットホームに依存しないＸＭＬ形式で記述される。セキュリティサーバー２０は、記述されたＤＳＰ２００をＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）、ＦＤ（Ｆｌｏｐｐｙ（登録商標）　Ｄｉｓｋ　Ｃｏｎｔｒｏｌｌｅｒ）、ＭＯ（Ｍａｇｎｅｔ　Ｏｐｔｉｃａｌ）、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ　Ｒｅａｄ－Ｏｎｌｙ　Ｍｅｍｏｒｙ）等の記録媒体１０２へ格納する（ステップＳ２）。また、セキュリティサーバー１０１は、ネットワーク１を介してＤＳＰ２００をプリンタ４０、複合機５０の入出力装置１０へ伝送する。

【００９１】

従って、ＤＳＰ２００が格納された記録媒体１０２を各入出力装置１０に配布し、また、ネットワーク１を介してＤＳＰ２００を伝送することにより一貫したＤＳＰ２００を各入出力装置１０に反映させることができる。

【００９２】

尚、セキュリティサーバー１０１では、ＤＳＰ２００をディスプレイ等の表示ユニットに表示することにより、ＤＳＰ２００の記述及び設定変更が行われる。また、セキュリティサーバー１０１が有する補助記憶装置等にＤＳＰ２００を格納するようにしてもよい。

【００９３】

尚、記録媒体１０２は、上記記録媒体に限定されることなく、ＤＳＰ２００を記録することができ、コンピュータが読み取り可能な媒体であれば適応可能である。

【００９４】

尚、上記複合機５０のかわりにコピー機を用いるようにしてもよい。

【００９５】

このように、上記ドキュメントセキュリティプロファイル方法において、プリンタ４０から受信した文書のセキュリティに関する文書属性情報に基づいて、文書のコンテンツに埋め込まれる埋め込み情報をプリンタ４０に送信し、複合機５０から受信した埋め込み情報に基づいて、文書属性情報を複合機５０に送信することにより、文書に関するセキュリティ情報を送受信して複数の入出力装置のセキュリティを統括して管理し、そのセキュリティを反映させた文書に関する処理を行うことができる。

【００９６】

また、文書を識別する文書ＩＤに対応付けて文書属性情報と埋め込み情報とを文書情報として管理する文書情報ＤＢ３１を有することにより、効率的に文書のセキュリティに関する情報を参照してプリンタ４０や複合機５０への送受信を行うことができる。

【００９７】

また、埋め込み情報が文書を一意に識別するバーコード情報、透かし情報、地

紋情報のうち少なくとも一つの情報であることにより、埋め込み情報で文書のコンテンツや文書属性を識別して文書に関する処理が実行されるため、文書のセキュリティを確保することができる。

【００９８】

【発明の効果】

上述の如く本発明によれば、第１の入出力装置から受信した文書のセキュリティに関する文書属性情報に基づいて、文書のコンテンツに埋め込まれる埋め込み情報を第１の入出力装置に送信し、第２の入出力装置から受信した埋め込み情報に基づいて、文書属性情報を第２の入出力装置に送信することにより、文書に関するセキュリティ情報を送受信して複数の入出力装置のセキュリティを統括して管理し、そのセキュリティを反映させた文書に関する処理を行うことができる。

【図面の簡単な説明】

【図１】

本発明の第１実施例に係る入出力装置のハードウェア構成を示すブロック図である。

【図２】

本発明の第１実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図３】

本発明の第２実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図４】

文書情報ＤＢに格納されたテーブルを示す図である。

【図５】

本発明の第３実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図６】

本発明の第４実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図７】

本発明の第５実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図８】

本発明の第６実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図９】

本発明の第７実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図１０】

本発明の第８実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図１１】

本発明の第９実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図である。

【図１２】

ドキュメントに関するセキュリティポリシーの例を示す図である。

【図１３】

ＤＳＰの識別情報を示す図である。

【図１４】

ＤＳＰの記述例を示す図である。

【図１５】

ＤＳＰの記述例を示す図である。

【図１６】

ドキュメントセキュリティポリシーの記述方法におけるシステム構成図である。

【符号の説明】

１　　ネットワーク

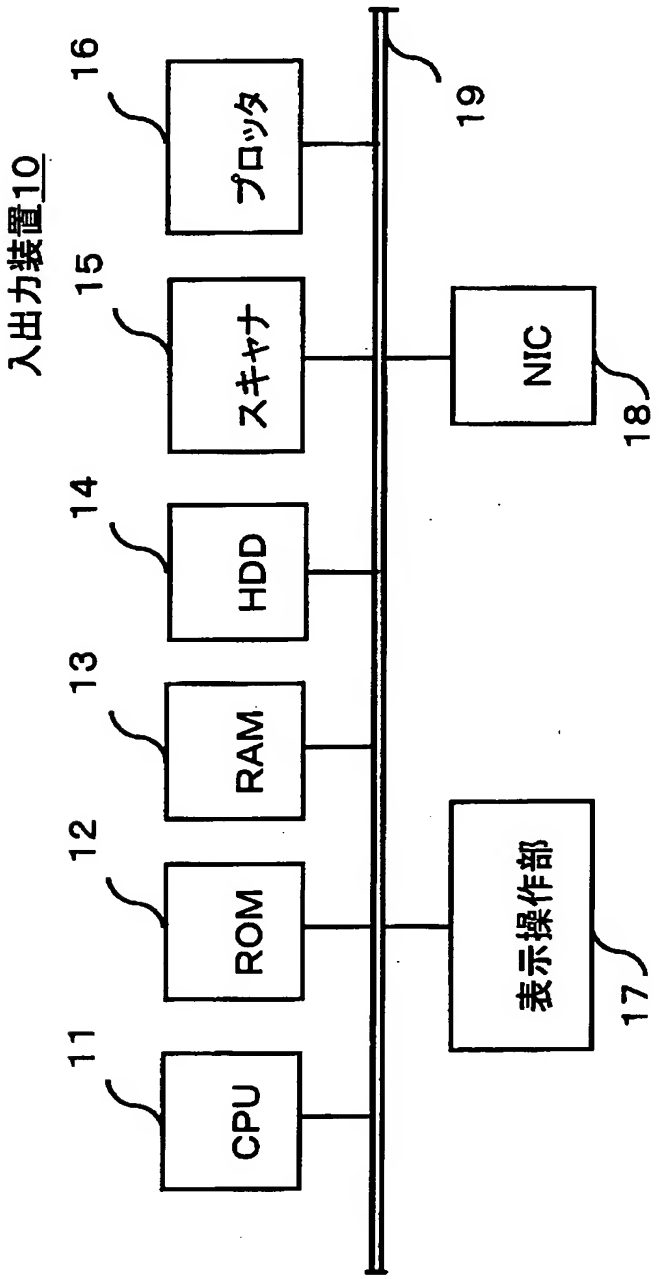
２～８、８０、８００　ドキュメントセキュリティシステム

１０	入出力装置
１１	ＣＰＵ
１２	ＲＯＭ
１３	ＲＡＭ
１４	ＨＤＤ
１５	スキャナ
１６	プロッタ
１７	表示操作部
１８	ＮＩＣ
１９	バス
２０、２１、２２	文書処理部
２５、２６	ＰＤＦファイル
３０、３２	ドキュメントセキュリティプロファイル処理部
３１	文書情報ＤＢ
３５	プラグイン
４０	プリンタ
５０、５１	複合機
６０	紙
６１	埋め込み情報
７０、７１	アダプタ
１００	セキュリティ管理システム
１０１	セキュリティサーバー
１０２	記録媒体
２００	ドキュメントセキュリティポリシー

【書類名】　図面

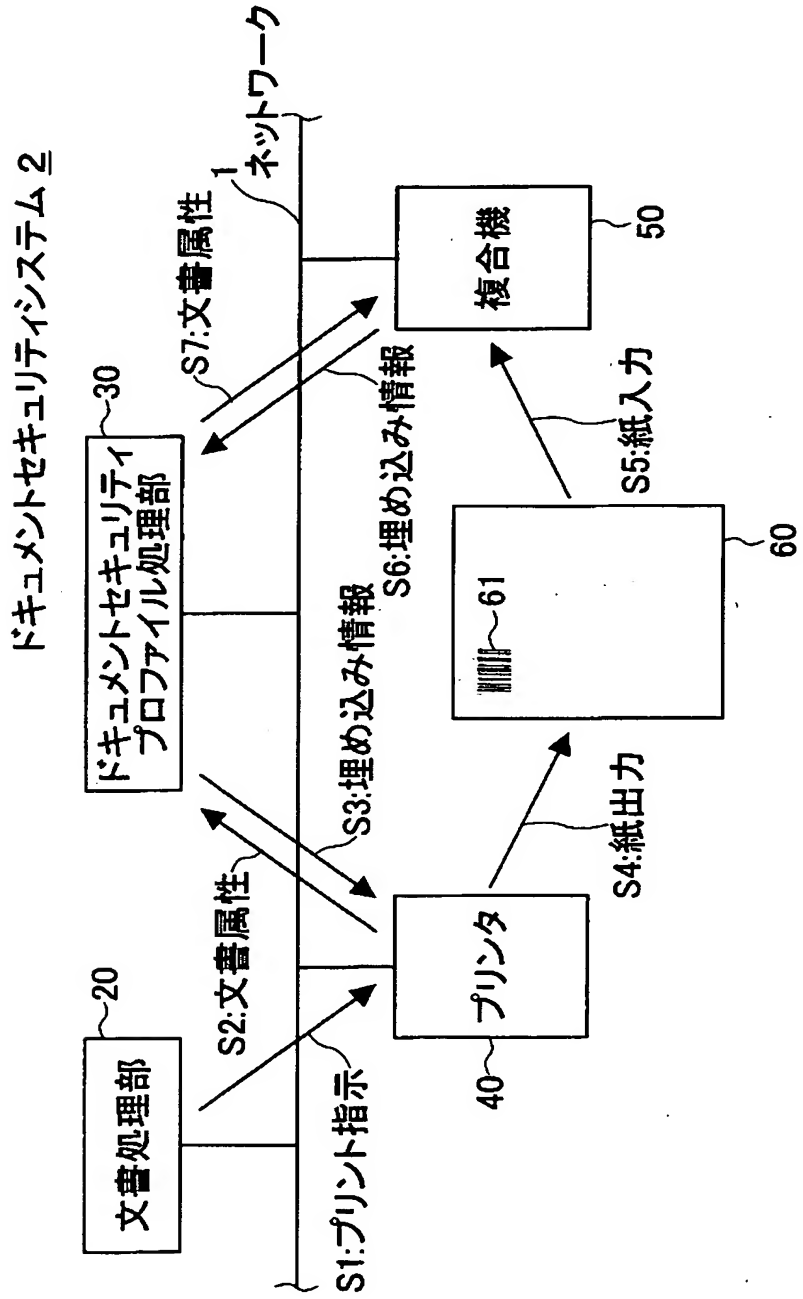
【図１】

本発明の第１実施例に係る入出力装置の
ハードウェア構成を示すブロック図



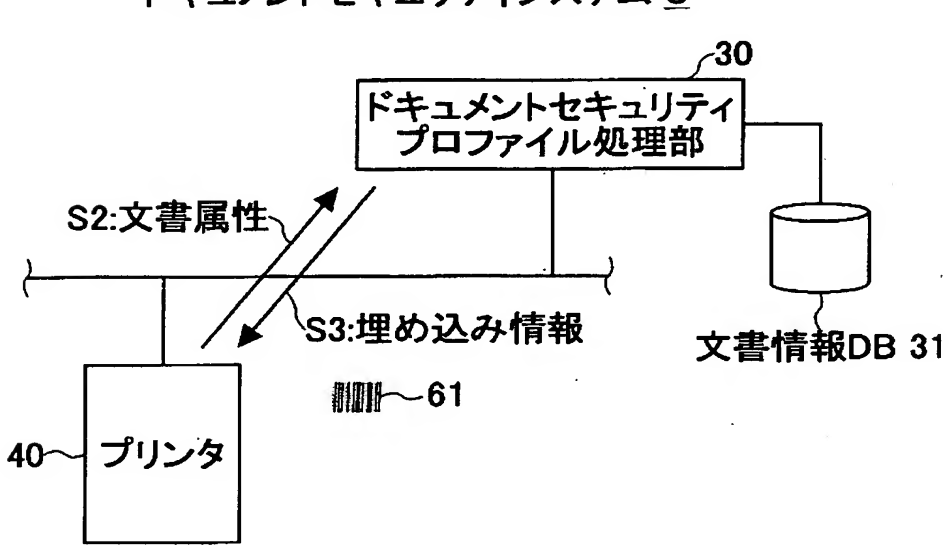
【図２】

本発明の第１実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図



【図３】

本発明の第2実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図



【図４】

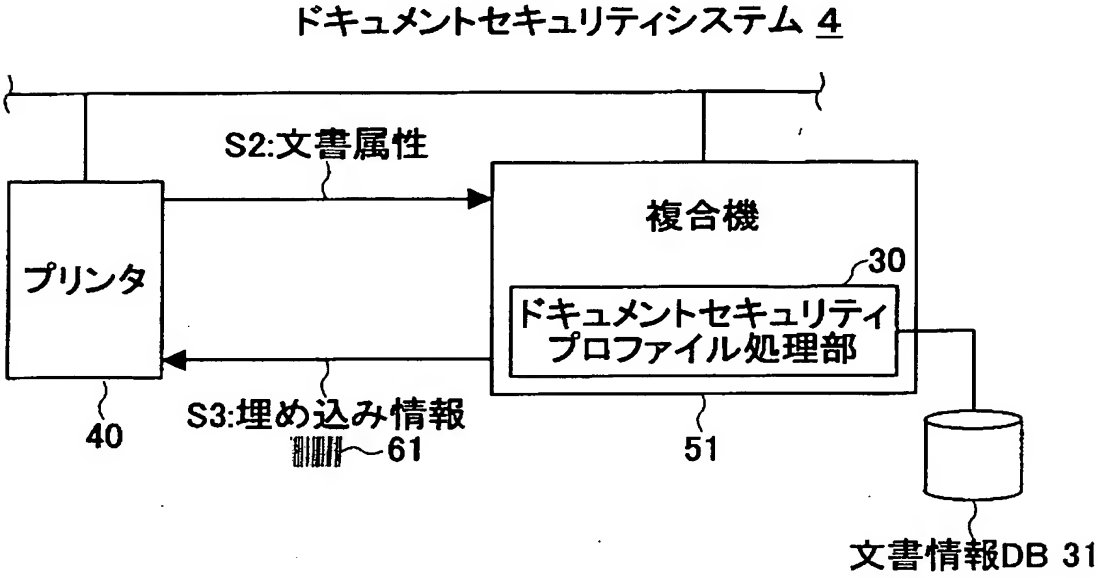
文書情報DBに格納されたテーブルを示す図

310

文書ID	文書属性ファイル	埋め込み情報
0238-20020730-1001	Attribute-23981.txt	Bar01010.bmp
0238-20020730-1002	Attribute-98263.txt	Bar01020.bmp
0238-20020730-1003	Attribute-37482.txt	Bar01030.bmp
0238-20020730-1004	Attribute-38471.txt	Bar01040.bmp

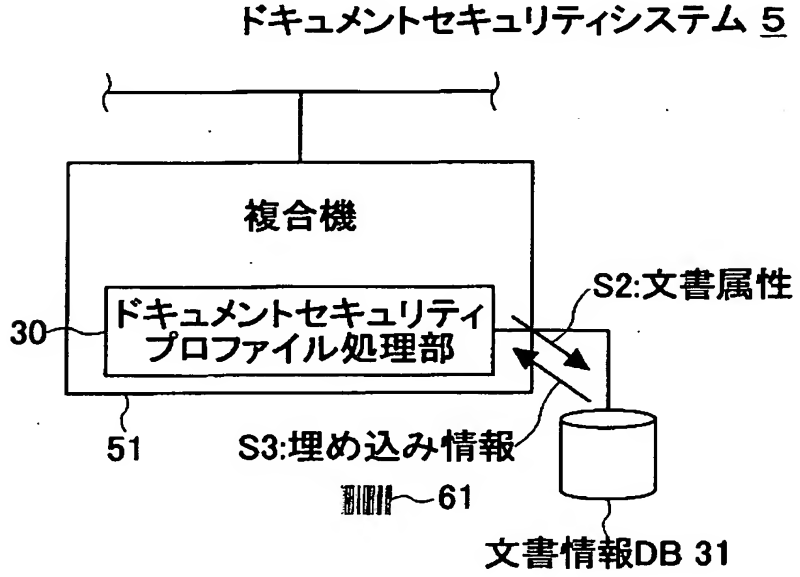
【図５】

本発明の第3実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図



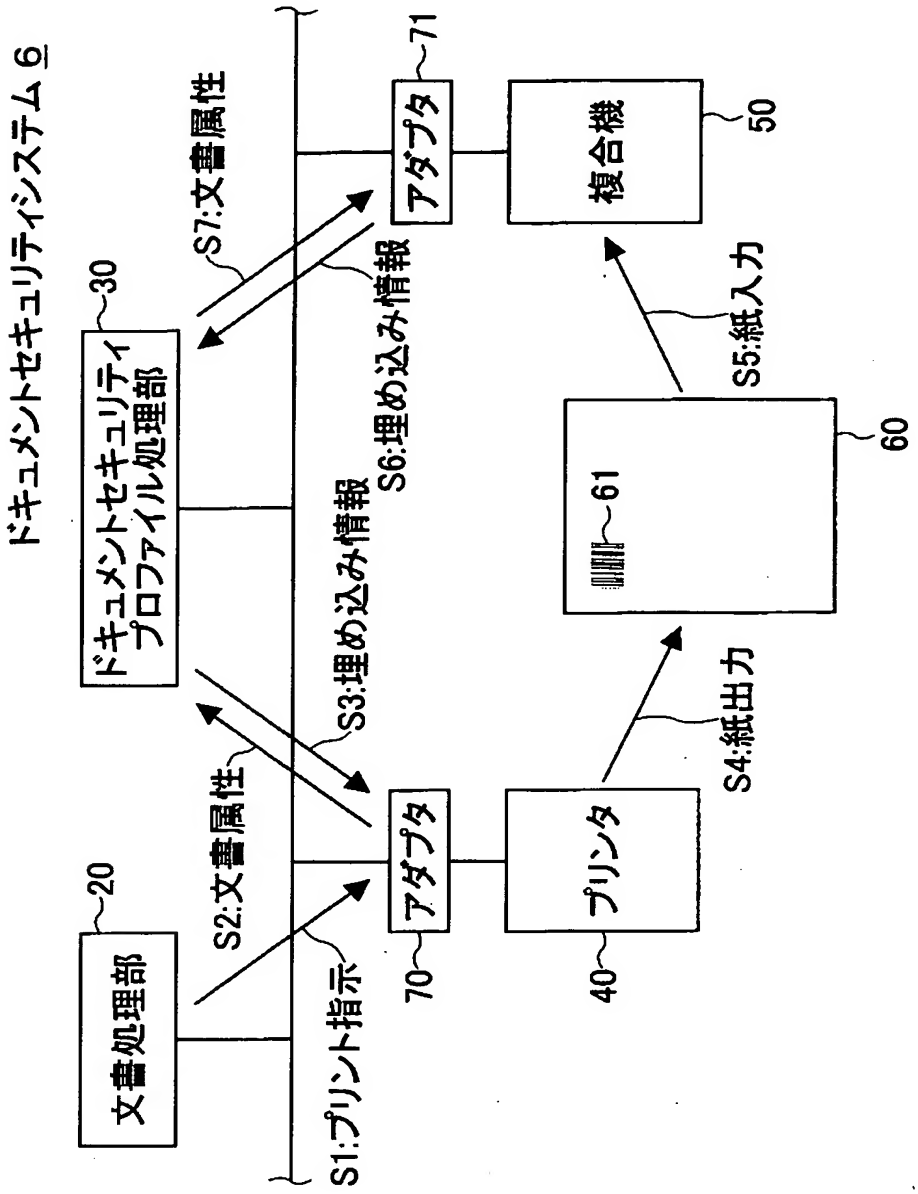
【図６】

本発明の第4実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図



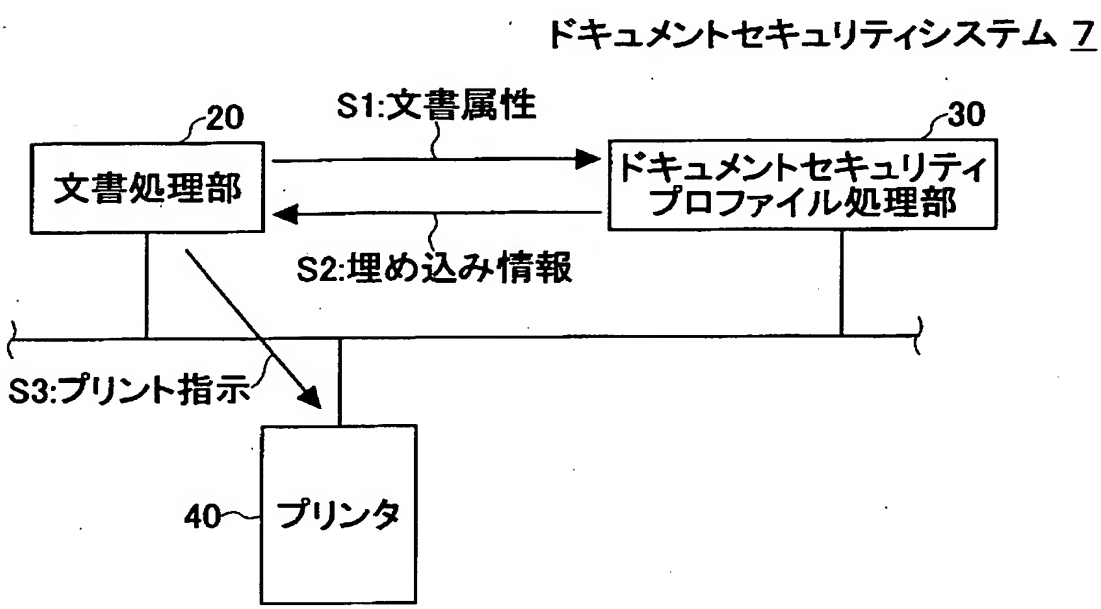
【図７】

本発明の第5実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図



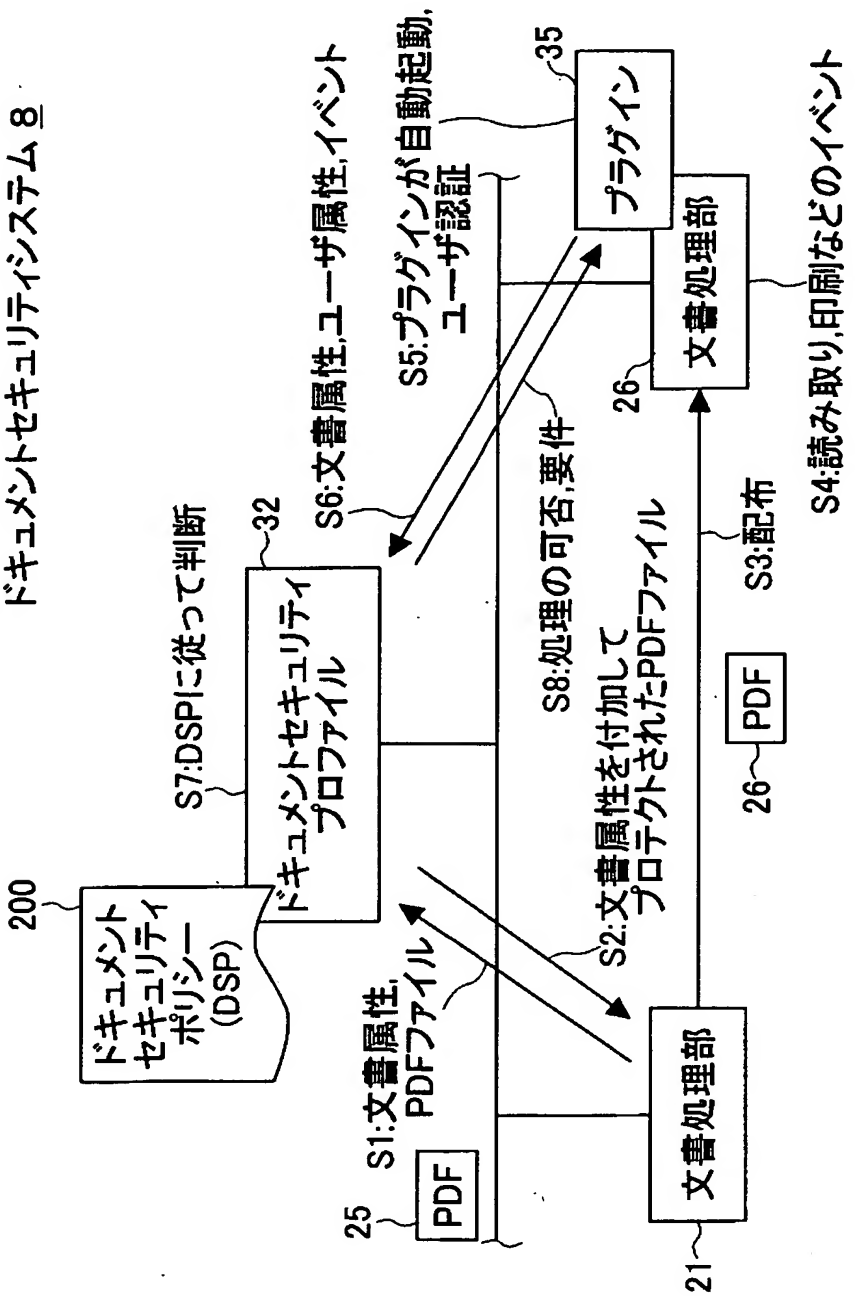
【図８】

本発明の第6実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図



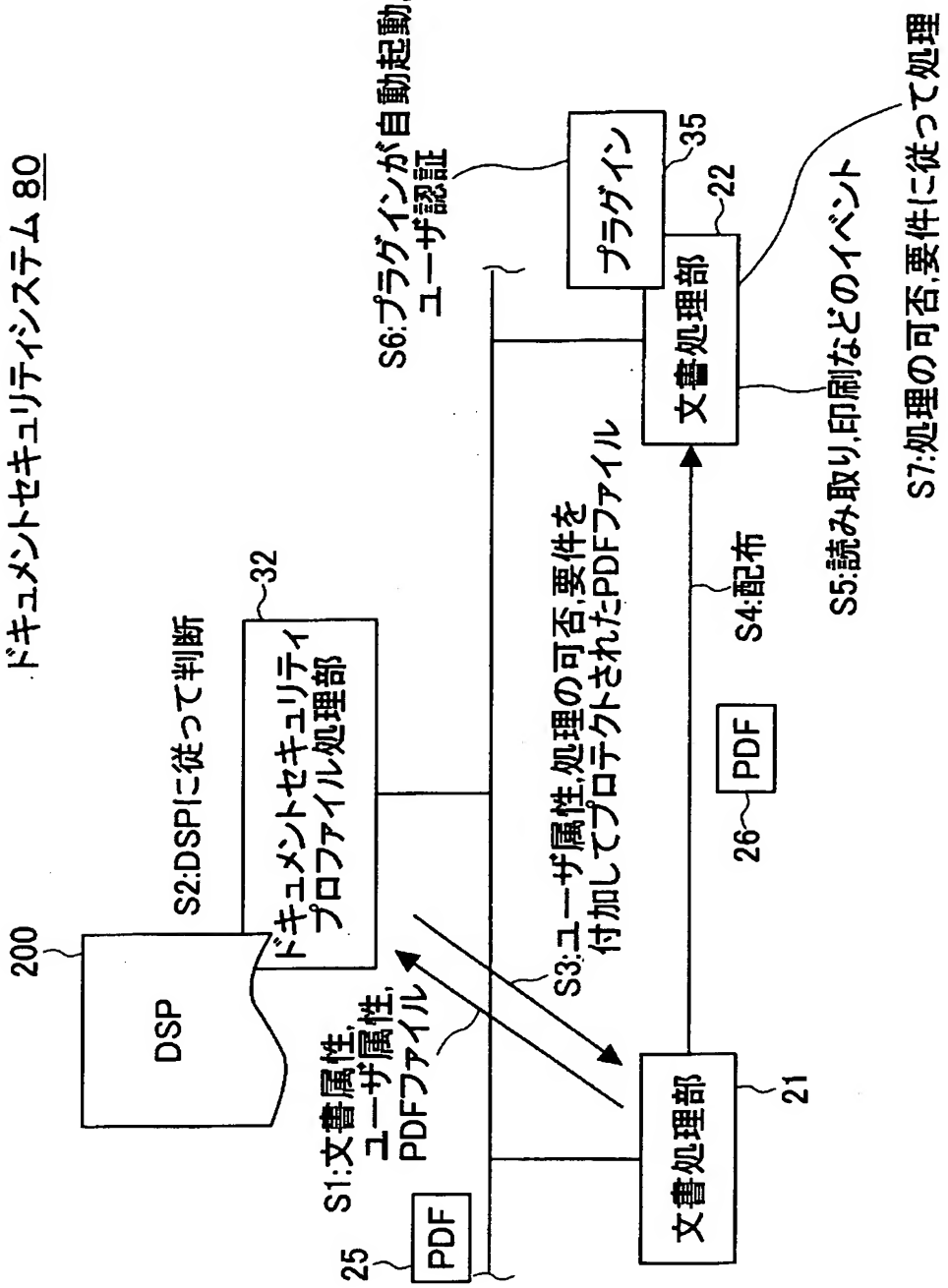
【図９】

本発明の第7実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図



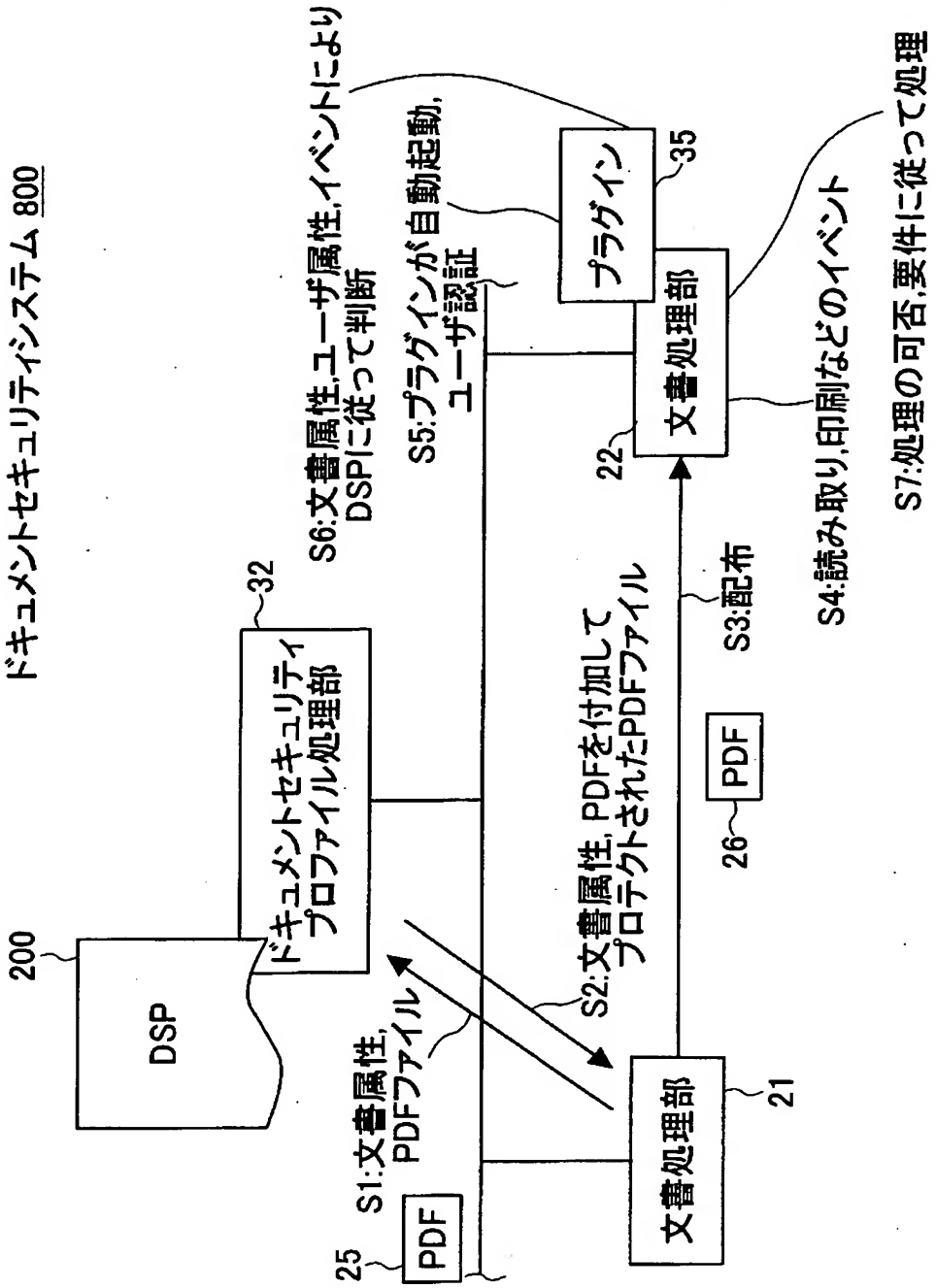
【図１０】

本発明の第8実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図



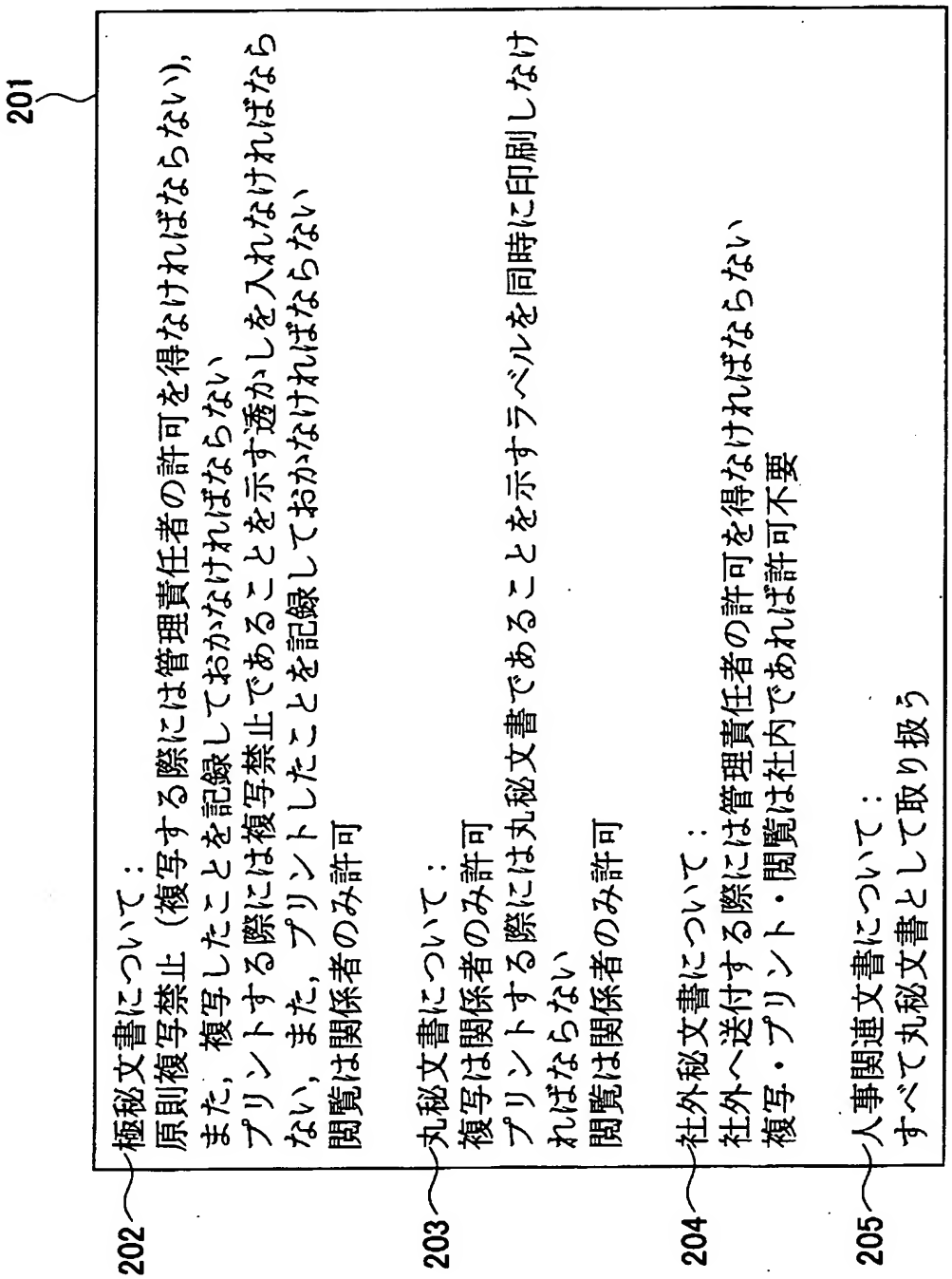
【図１１】

本発明の第9実施例に係るドキュメントセキュリティプロファイル方法におけるシステム構成図



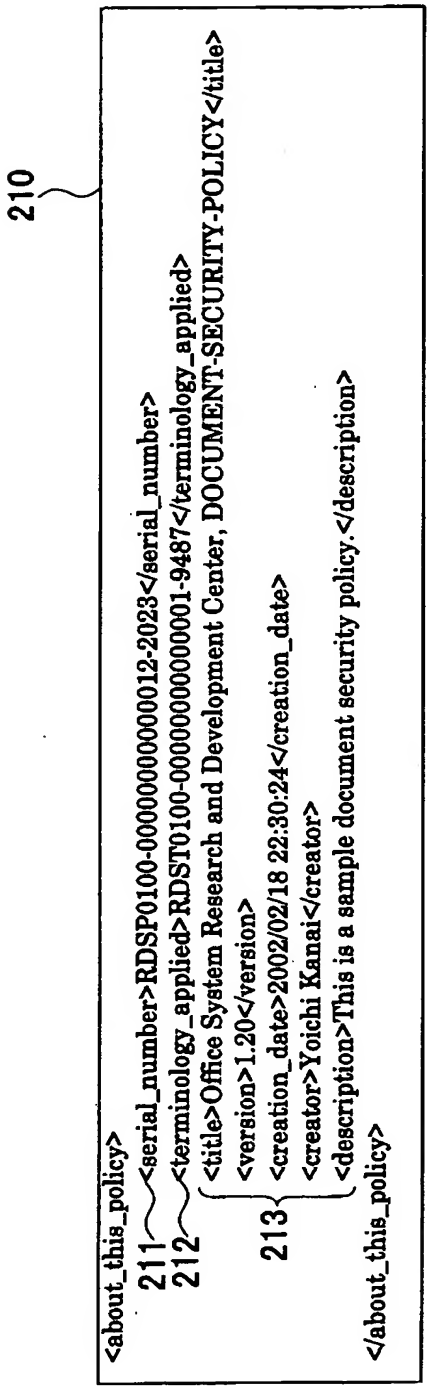
【図１２】

ドキュメントに関するセキュリティポリシーの例を示す図



【図１３】

DSPの識別情報を示す図



【図１４】

DSPの記述例を示す図

220

```
<policy>
 221～<acc_rule>
       222～<doc_category>ANY</doc_category>
            <doc_security_level>medium</doc_security_level>
         223～<acl>
                 224～<ace>
                         225～<user_category>DOC-CATEGORY
                              </user_category>
                         226～<user_security_level>ANY
                              </user_security_level>
                         227～<operation>
                                 228～<name>fax_send</name>
                                 229～<denied/><!-- denied even if it
                                        is explicitly authorized -->
                              </operation>
                         227～<operation>
                                        <name>net_delivery</name>
                                 230～<requirement>audit
                                        </requirement>
                                 231～<requirement>
                                              explicit_authorization
                                        </requirement>
                                        ...
                              </operation>
                         227～<operation>
                                        <name>fax_receive</name>
                                 231～<allowed/><!--allowed
                                        without requirements -->
                              </operation>
                              ...
                       </ace>
                 224～<ace>
                              ...
                       </ace>
               </acl>
       </acc_rule>
 221～<acc_rule>
               <doc_category>ANY</doc_category>
               <doc_security_level>high</doc_security_level>
               <acl>
                       ...
               </acl>
       </acc_rule>
</policy>
```

【図１５】

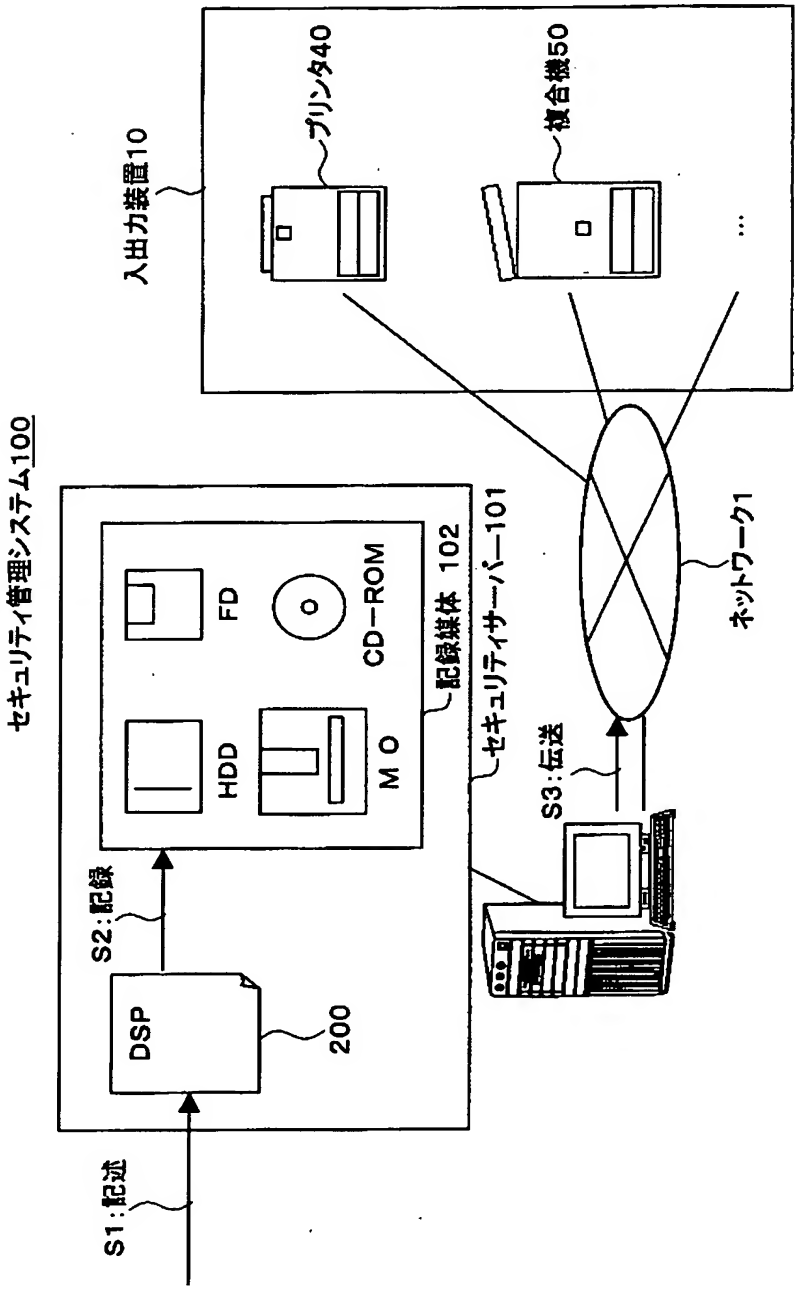
DSPの記述例を示す図

240

```
<policy>
    <acc_rule>
        <doc_category>ANY</doc_category>
        <doc_security_level>medium</doc_security_level>
        <acl>
            <ace>
                <user_category>DOC-CATEGORY</user_category>
                <user_security_level>ANY</user_security_level>
241 ~~<denied_operations> <!-- denied even if it is explicitly
                                    authorized -->
                    <name>fax_send</name>
                </denied_operations>
                <operation>
                    <name>net_delivery</name>
                    <requirement>audit</requirement>
242 ~~<requirement>explicit_authorization
                    </requirement>
                                ...
                </operation>
                <operation>
                                ...
                </operation>
243 ~~<allowed_operations> <!-- allowed without
                                    requirements -->
                    <name>fax_receive</name>
                    <name>store</name>
                                ...
                </allowed_operations>
            </ace>
            <ace>
                        ...
            </ace>
                        ...
        </acl>
    </acc_rule>
    <acc_rule>
        <doc_category>ANY</doc_category>
        <doc_security_level>high</doc_security_level>
        <acl>
                    ...
        </acl>
    </acc_rule>
</policy>
```

【図１６】

ドキュメントセキュリティポリシーの
記述方法におけるシステム構成図



【書類名】　　要約書

【要約】

【課題】　文書に関するセキュリティ情報を送受信して複数の入出力装置のセキュリティを統括して管理し、そのセキュリティを反映させた文書に関する処理を行うことができるドキュメントセキュリティプロファイル方法を提供することを目的とする。

【解決手段】　本発明の課題は、入出力装置との文書のセキュリティに関する情報の送受信を制御するドキュメントセキュリティプロファイル方法であって、第１の入出力装置から受信した文書のセキュリティに関する文書属性情報に基づいて、上記文書のコンテンツに埋め込まれる埋め込み情報を上記第１の入出力装置に送信する第１送受信手順と、第２の入出力装置から受信した上記埋め込み情報に基づいて、上記文書属性情報を上記第２の入出力装置に送信する第２送受信手順とを有する構成とされる。

【選択図】　　図２

特願２００２－３４１２２２

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都大田区中馬込１丁目３番６号
氏　名　株式会社リコー

２．変更年月日　　２００２年　５月１７日
［変更理由］　住所変更
住　所　東京都大田区中馬込１丁目３番６号
氏　名　株式会社リコー